Raytheon
BBN Technologies

BBN Technologies
10 Moulton Street
Cambridge, MA 02138

25 April 2014

Office of Naval Research
875 North Randolph Street, Suite 1179
Arlington, VA 22203-1995

Delivered via Email to:
carey.schwartz@navy.mil
reports@library.nrl.navy.mil
tr@dtic.mil
shannon.viverette@navy.mil

Contract Number:	N00014-14-C-0002
Proposal Number:	P13003-BBN
Contractor Name and PI:	Raytheon BBN Technologies; Dr. Jonathan Habif
Contractor Address:	10 Moulton Street, Cambridge, MA 02138
Title of the Project:	Seaworthy Quantum Key Distribution Design and Validation (SEAKEY)
Contract Period of Performance:	7 February 2014 – 7 February 2016
Total Contract Amount:	$475,359 (Base)
Amount of Incremental Funds:	$123,437
Total Amount Expended (thru 11 April):	$29,484

Attention: Dr. Carey Schwartz
Subject: Quarterly Progress Report
Reference: Exhibit A, CDRLs

In accordance with the reference requirement of the subject contract, Raytheon BBN Technologies (BBN) hereby submits its first Quarterly Progress Report. This cover sheet and enclosure have been distributed in accordance with the contract requirements.

Please do not hesitate to contact Dr. Habif at 617.873.5890 (email: jhabif@bbn.com) should you wish to discuss any technical matter related to this report, or contact the undersigned, Ms. Kathryn Carson at 617.873.8144 (email: kcarson@bbn.com) if you would like to discuss this letter or have any other questions.

Sincerely,
Raytheon BBN Technologies

Kathryn Carson
Program Manager
Quantum Information Processing

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
25 APR 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Seaworth Quantum Key Distribution Design and Validation (SEAKEY)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Raytheon BBN Technologies,10 Moulton Street,Cambridge,MA, 02138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

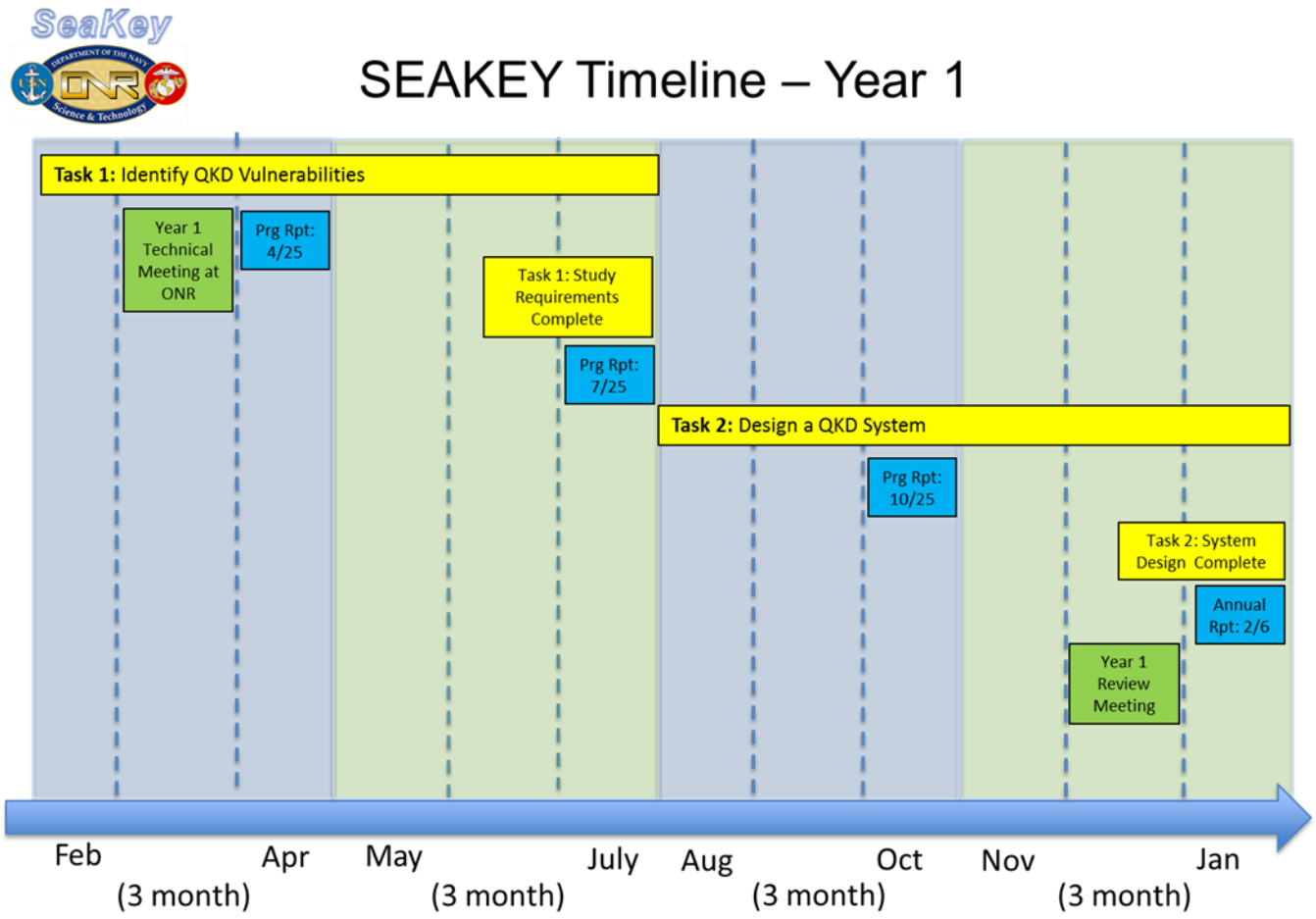
15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**10**	

SEAKEY Quarterly Progress Report for the
Period 7 February 2014 – 25 April 2014 (100 Days)

Section A. Project Schedule

The Year 1 timeline below identifies SeaKey tasks, their duration, task milestones, kickoff meeting, tentative program review meeting, and progress report due dates.



Section B. Technical Progress

SUMMARY

In this report we summarize the technical progress accomplished during the first quarter of work of the SeaKey program. We describe our information theoretic work to define the performance bounds of QKD systems operating under ideal scenarios, and how those bounds guide our path forward for link design. We also describe our progress

quantifying the non-idealities that will be encountered in a free-space optical (FSO) link operating in a marine environment.

INTRODUCTION

Our work, to date, has spanned two major efforts: (1) calculating maximum secret key rate capacities for idealized, quantum key distribution (QKD) systems operated in a lossy, free-space channel, and (2) determining the non-idealities that will be encountered operating an optical communications link in a free-space channel through a marine environment.

In our modeling work we compared CV-QKD performance against that achievable with BB84 protocols. In a previous updated, we reported that in a pure-loss channel (with all other parameters idealized), BB84 performs very close to the bounds of the best achievable QKD protocols. We have assembled modeling programs that will allow us to compare CV-QKD against BB84 protocols as we begin introducing non-idealities into the model.

Understanding the non-idealities that we will eventually hinder FSO communications in a marine environment is critical to understanding the hardware that needs to be identified and/or developed to implement a QKD link. In the following technical summary, we present the results of our literature survey quantifying the atmospheric attenuation that will be present in a marine environment due to scattering and absorption from aerosols in a marine environment. We also present a mixture of data gathered from a literature survey, as well as initial calculations quantifying the radiance that we can expect from solar light scattered by the sky, as well as blackbody radiation generated by the earth (dominant at longer wavelengths). Derived from the data we have gathered thus far, we present a set of operating wavelengths that we initially deem as having high potential for fielding a QKD system. Specifically, wavelengths of 2.2 μm and 3.7 μm are identified as having the highest potential for operating wavelengths because they lie in spectra with low aerosol absorption, and minimized background radiance from scattered solar, and blackbody radiation. Importantly, we point out that the analyses performed thus far do not include non-idealities due to atmospheric turbulence. We are anticipating that longer wavelengths will suffer less scintillation in a turbulent environment, and thus, have disregarded shorter wavelengths as high-value candidates for FSO QKD implementation.

METHODS, ASSUMPTIONS AND PROCEDURES

Our work modeling QKD systems has thus far assumed: perfect single photon sources at the transmitter, and losses due to beam diffraction, turbulence induced scintillation, and sub-unit system efficiency at our receiver.

The data that we have found to provide input to our atmospheric modeling work was derived from a number of sources that we cite within this report. Notably, data was derived from ***The Infrared Handbook*** [1] and other resources for archived data. Figure 1 shows a distribution of aerosol particle sizes in the marine environment [2]. The distribution is bi-modal, and has a strong influence on the wavelength dependence of scattering, shown in later figures.

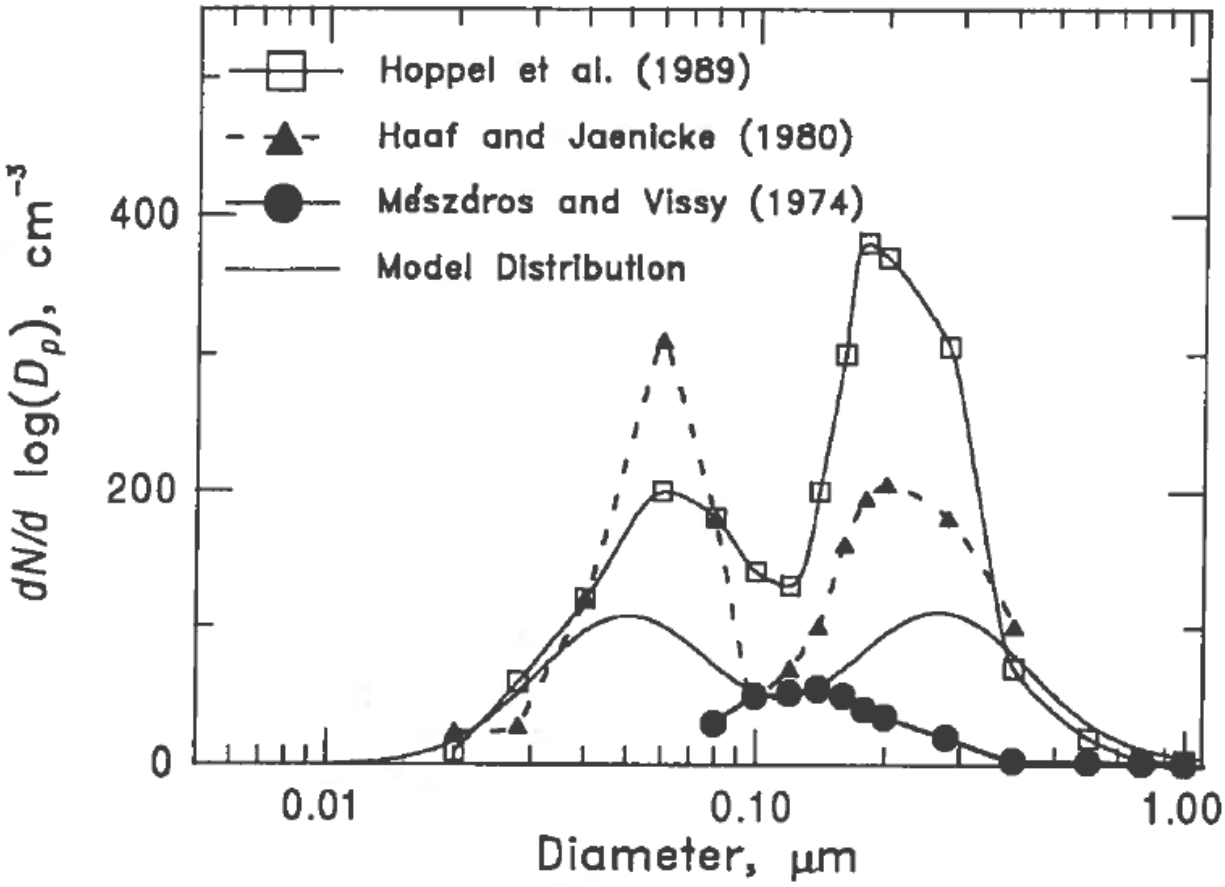


Figure 1 Distribution of particulate aerosols in the marine atmosphere. Taken from [2].

	Clean Continental		Urban		Maritime	
Wl (nm)	Real	Imaginary ($\times 10^{-3}$)	Real	Imaginary ($\times 10^{-2}$)	Real	Imaginary ($\times 10^{-4}$)
300.0	1.530	−8.00	1.535	−1.82	1.402	−4.01
400.0	1.530	−6.56	1.535	−1.50	1.392	−2.50
550.0	1.530	−7.04	1.535	−1.56	1.388	−3.00
694.0	1.530	−7.52	1.535	−1.63	1.384	−3.50

Figure 2 Wavelength dependence of the indices of refractions for different aerosol composition environments.

Derived from the data in Figure 1, is the index of refraction for a medium with mixed aerosols. The real part of the index is associated with scattering and the imaginary part of the index is associated with absorption. It is seen that scattering is dominant in a marine environment, at least in the visible wavelength range shown in the data. This data is used to generate the curve shown in figure 3 taken from [1]. Notably, from this figure, there is an inverse relation between wavelength and attenuation coefficient indicating that increased wavelength should enable improved transmission performance for a FSO link.

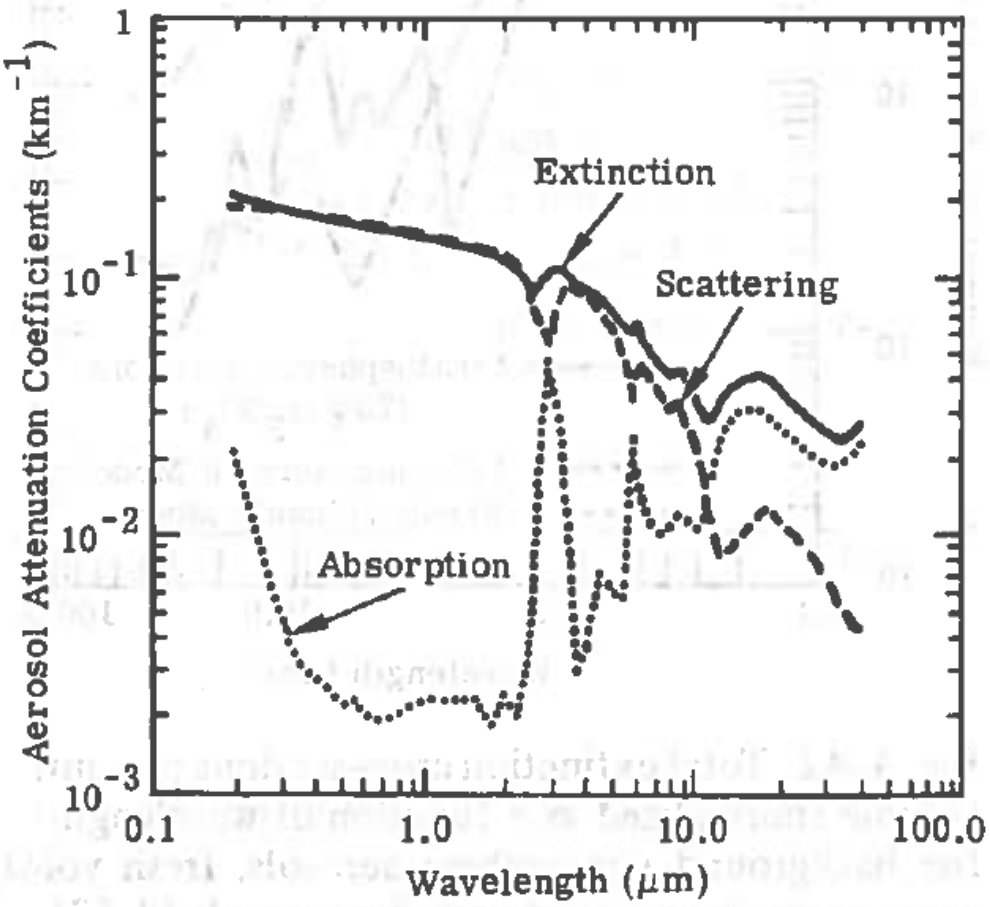


Figure 3 Attenuation coefficient as a function of wavelength due to aerosol scattering and absorption [1].

RESULTS AND DISCUSSIONS

In our modeling effort we compared CV-QKD with Gaussian modulation against the more standard BB84 protocols We found that the secret key rate for CV-QKD with Gaussian modulation scales as well as BB84 (can overcome the worse scaling of BB84) in the presence of loss. Also, CV-QKD with an appropriate PSK or QAM modulation can approach the performance of the full Gaussian distribution, which is likely not practical

to implement, but often considered in theoretical analyses. We are working on evaluating key rates for this protocol.

Our modeling work also found that BB84 with polarization-coded laser light, without decoy states scales the same way (poorly) as BPSK-CV QKD. Decoy states improves performance, brings up the rate-distance scaling to single-photon BB84, but is worse by a factor of 2 to 4 in actual rate. There could still be rate advantage (over single-photon BB84), however, due to higher modulation bandwidth of laser transmitter than single photon source.

We have also begun evaluating security issues in FSO QKD systems. In discussions with Norbert Lutkenhaus, Saikat Guha found a fundamental difference between the rates of direct-secure communication and QKD. The former is higher with same modulation and detection assumptions, because of assumed channel knowledge. They are working to resolve this matter, as this has been a source of debate in the quantum security community.

Finally, we analyzed the efficacy of using multiple spatial modes, and based on parameter space suggested by sponsor, determined than using up to (but not more than) ~4 spatial modes could be beneficial. System at the brink of near and far field propagation. We are currently evaluating key rates for the multi-mode case.

In conjunction with the aerosol scattering and absorption data presented in the previous section, we have plotted the background radiance that we can expect in an FSO link as a function of wavelength in figure 4. Radiant background will enter the QKD receiver as noise, causing an increased quantum bit error rate (QBER) reducing the achievable secret key rate. The radiance data in figure 4 shows contributions from both scattered solar radiance in the sky, as well as radiance generated by a 300K blackbody generated by the earth. From figure 4 we can see that there is a minimum of the background radiance in the wavelength band between 2.2 μm and 4 μm. Also plotted in this figure is the transmissivity of air, and it is apparent that there are relatively narrow windows of the spectrum with high transmissivity. Therefore, with the current data we believe that operating at either 2.2 μm or 3.7 μm could yield improved transmission in the marine FSO channel.

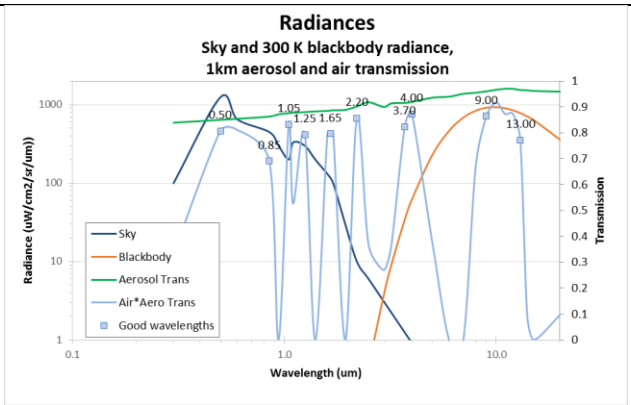


Figure 4 Atmospheric transmissivity data combined with background radiance data to determine recommended wavelengths for operation of a FSO link for QKD [4].

RECOMMENDATIONS

Our modeling work has benefited from discussions with Professor Jeff Shapiro on turbulence effects in QKD systems. Saikat Guha met with Jeff Shapiro, and went over detailed modeling of atmospheric scatterers and fading due to scintillation and log-normal fading. Saikat is currently evaluating secret key rates for BB84 with decoy and CV-QKD with multi-level PSK modulation. Jeff suggested looking into transmission of LO-reference beacon for Saikat's CV-QKD-under-turbulence rate calculation. This is an interesting suggestion, since one big downside of CV-based QKD is the spatial and temporal mode matching of the LO, which doesn't come into play for a polarization-coded single-mode BB84.

Moving forward we plan to analyze adaptive-optics approaches for spatial mode tracking for the homodyne LO for CV protocol, and plan to analyze key-rate improvement using reciprocity-enhanced model, which has been shown to improve direct communication rate.

We plan to examine currently available hardware systems for their compatibility with a QKD testbed:

- The NovaSol free-space optical communications interrogator offers position, acquisition and tracking capability at 1.5 µm in a single compact box. Novasol and Exelis Technologies have also developed the Tactical Line-of-Sight Optical Network (TALON) free-space optical communications system, which has been tested over distance of 50 km in a naval environment. We have contacted Rick Holasek, the president of Novasol and will be scheduling a meeting with him over the spring/summer. In particular, we will study the robustness of the Novasol systems in the presence of oceanic waves and turbulence.
- LaserLight Communications is developing advanced technologies for space-based optical communications . We will investigate if such platforms would be useful for marine communication.

- We will also investigate the multiple quantum-well and InGaAs modulating retroreflectors developed by NRL for their compatibility with a free-space QKD system.

Contact SPAWAR for corroboration of the data that we have found, thus far, detailing non-idealities for optical propoagation in a free-space, marine environment including:

- Turbulence
- Atmospheric transmission
- Sky and blackbody radiance values
- Find and model more marine aerosol data
    - Polluted marine
    - Extinction spectra
    - Size distribution
- Acquire high resolution atmospheric transport code
    - MODTRAN or the like
- Calculate transmission versus wavelength and range
    - Atmospheric parameters, aerosol parameters, sensor properties
- More detailed calculations of background power vs wavelength
    - Sky background, thermal background
    - Evaluate effects of filter bandwidth and receiver Field of view

REFERENCES

1. William Wolfe and George Zissis, **Infrared Handbook,** Office of Naval Research, Department of the Navy, Washington DC (1985).
2. John Seinfeld and Spiros Pandis, **Atmospheric Chemistry and Physics**, Wiley, Hoboken, NJ (2006).
3. http://www.gps.caltech.edu/~vijay/Papers/Aerosol/levoni_guzzi.pdf
4. http://misclab.umeoce.maine.edu/education/VisibilityLab/reports/SIO_60-29.pdf

C. Problem Areas – Identification

There are no anticipated problems or issues to report at this time.

Section D. SEAKEY Financial Update

Financial Chart reflecting Year 1: